IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Robin Pou et al.	Art Unit	: 3621
Serial No.	: 10/726,284	Examiner	: John M. Winter
Filed	: December 2, 2003	Conf. No.	: 5291
Title	: DISTRIBUTION AND RIGHTS MANAGEMENT OF DIGITAL CONTENT		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF (37 CFR 41.37) OF JUNE 21, 2010

In response to the Notification of Non-Compliant Appeal Brief dated June 21, 2010, Appellants respectfully submit a replacement Appendix of Claims to correct Claim 49 to reflect the last entered amendment. Appellants believe that this replacement Appendix satisfies the requirements of 37 C.F.R. § 41.37.

Applicants believe no fees to be due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to deposit account 06-1050.

Respectfully submitted,

Date: June 25, 2010

/Jonathan A. Solomon/
Jonathan A. Solomon
Reg. No. 64,869

Customer Number 26231
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: June 25, 2010.

Replacement Appendix of Claims

49. A method for managing digital rights, the method comprising:

monitoring an input/output system of a user device for attempted file transfers between the user device and an external device through one or more input/output ports of the user device;

detecting an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file; and

applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device.

50. The method of claim 49 wherein the data file comprises a media file.

51. The method of claim 49 further comprising identifying the data file as embodying a particular protected work from a plurality of predetermined works, wherein the digital wrapper is applied based on the identity of the data file.

52. The method of claim 51 wherein the digital wrapper is applied based on the identity of the data file matching an identification of the data file in a database on the user device.

53. The method of claim 51 wherein identifying the data file comprises using a file recognition algorithm adapted for identifying data files as embodying particular protected works based on characteristics of the data files.

54. The method of claim 49 wherein the digital wrapper includes information identifying the data file and information relating to an allocation of credits to one or more distributors of the data file based on purchases of the data file.

60. A method for managing digital rights, the method comprising:

identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution;

identifying access rules associated with the media file, wherein the access rules include information relating to usage rights and usage fees;

applying a digital wrapper to the media file before distribution occurs, with the digital wrapper including identification data for the media file and data relating to the access rules, wherein the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device.

61. The method of claim 60 wherein the digital wrapper is adapted to be disabled for use of the media file by an external device that has a license to access the media file.

62. The method of claim 60 wherein the digital wrapper further includes information relating to at least one distributor of the media file.

100. An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

monitoring an input/output system of a user device for attempted file transfers between the user device and an external device through one or more input/output ports of the user device;

detecting an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file; and

applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device.

101. The article of claim 100 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising identifying the data file as being subject to protection from unauthorized copying.

102. The article of claim 101 wherein identifying the data file as being subject to protection from unauthorized copying includes locating an identifier for the data file in a database stored on the user device.

103. The article of claim 101 wherein identifying the data file as being subject to protection from unauthorized copying includes:

sending a message including information for identifying the data file to a remote server; and

receiving a response to the message indicating that the data file is subject to protection from unauthorized copying.

108. An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution;

identifying access rules associated with the media file, wherein the access rules include information relating to usage rights and usage fees;

applying a digital wrapper to the media file before distribution occurs, with the digital wrapper including identification data for the media file and data relating to the access rules, wherein the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device.

109. The article of claim 108 wherein identifying the media file comprises identifying the media file using a file recognition algorithm.

110. The article of claim 108 wherein identifying the access rules associated with the media file comprises receiving access rules from a remote server.

111. The article of claim 108 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising:

receiving a request from a user of the external device for authorization to access the media file after distribution of the media file from the user device;

notifying a remote server of the request for authorization to access the media file by the external device; and

disabling the digital wrapper to allow access to the media file by the user of the external device.

112. The article of claim 108 wherein identifying the access rules associated with the media file comprises receiving the access rules from the user device.